Unveiling Security, Privacy, and Ethical Concerns of ChatGPT

Abstract

This paper delves into the realm of ChatGPT, an AI-powered chatbot that utilizes topic modeling and reinforcement learning to generate natural responses. Although ChatGPT holds immense promise across various industries, such as customer service, education, mental health treatment, personal productivity, and content creation, it is essential to address its security, privacy, and ethical implications. By exploring the upgrade path from GPT-1 to GPT-4, discussing the model's features, limitations, and potential applications, this study aims to shed light on the potential risks of integrating ChatGPT into our daily lives. Focusing on security, privacy, and ethics issues, we highlight the challenges these concerns pose for widespread adoption. Finally, we analyze the open problems in these areas, calling for concerted efforts to ensure the development of secure and ethically sound large language models.